

REMARKS

The Examiner is thanked for the performance of a thorough search.

Claims 1, 4-7, 21, 23-25, 27-29, 31-32, 34-37, 39-42, and 44-47 have been amended. No claims have been added or canceled. Hence, Claims 1, 4-21, 23-25, 27-29, 31-32, 34-37, 39-42, and 44-47 are pending in the present application.

Each issue raised in the Office Action mailed March 27, 2008 is addressed hereinafter.

I. ISSUES NOT RELATING TO THE PRIOR ART

A. REJECTIONS UNDER 35 U.S.C. § 101

Claims 21, 23-24, and 34-37 were rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. Specifically, the Office Action asserted that each of Claims 21, 23-24, and 34-37 seems to cover “transmission medium”, which the Office Action considers as non-statutory.

The Applicant disagrees that “transmission medium” as described in the specification is non-statutory. However, solely in order to further the prosecution of the present application, each of Claims 21, 23-24, and 34-37 has been amended herein to feature a “computer-readable volatile or non-volatile medium storing one or more sequences of instructions...”. Further, at least paragraph [0081] of the specification describes that non-volatile media may include, for example, optical or magnetic disks, and that volatile media may include dynamic memory. Thus, the “computer-readable volatile or non-volatile medium” featured in Claims 21, 23-24, and 34-37 is directed to statutory subject matter because optical disks, magnetic disks, and dynamic memory are clearly articles of manufacture.

For at least this reason, each of Claims 21, 23-24, and 34-37 is directed to statutory subject matter. Reconsideration and withdrawal of the rejections of Claims 21, 23-24, and 34-37 under 35 U.S.C. § 101 is respectfully requested.

B. REJECTIONS UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 1, 21, 25, and 29 were rejected as allegedly indefinite under 35 U.S.C. § 112, second paragraph. Specifically, the Office Action seems to assert that “two or more” of an entity cannot be included into “one or more “ of that entity. This assertion is logically incorrect because the term “one or more” is broader than, and includes, the term “two or more.” For example, if a person has “one or more” apples, it is abundantly clear that the person can have: two apples, or three apples, or four apples, etc.; thus, two apples or three apples or four apples are clearly “two or more” apples.

Nevertheless, solely in order to further the prosecution of the present application, each of Claims 1, 21, 25, and 29 has been amended herein to feature “two or more” digital signatures. Thus, reconsideration and withdrawal of the rejections of Claims 1, 21, 25, and 29 under 35 U.S.C. § 112, second paragraph is respectfully requested.

II. ISSUES RELATING TO THE CITED ART

A. INDEPENDENT CLAIM 1

Claim 1 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over Bosler, U.S. Patent Application Publication No. US 2005/0010757 (“BOSLER”) in view of Kinnis et al., U.S. Patent No. 6,959,382 (“KINNIS”). The rejection is respectfully traversed.

Among other features, Claim 1 comprises the features of:

receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals;

... ;

verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element;

applying the configuration directives to the host network element only when the two or more digital signatures are verified successfully;

wherein applying the configuration directives comprises **applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals.**

It is respectfully submitted that BOSLER and KINNIS do not describe or suggest the features of Claim 1 that are highlighted above.

The Office Action asserts that in paragraphs [0058] and [0069] BOSLER describes the features of Claim 1 of: receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. These assertions are incorrect.

In paragraph [0058], BOSLER describes that a first node and a second node may establish a secure session by exchanging a management message that may be authenticated by a digital signature. Specifically, BOSLER describes that the first node and the second node may establish a secure session by mutual authentication using their respective public keys. (Paragraph [0058], lines 9-12.) The first node may send a management message to the second node (paragraph [0058], lines 7-9), where the management message may be signed by a digital signature generated by using the first node's private key (paragraph [0058], lines 13-17). In paragraph [0069], BOSLER describes a management server that receives information from distributed agents on the nodes being managed, and that sends management requests to the agents.

Significantly, however, neither paragraph [0058] nor any other paragraph of BOSLER describes or suggests that a management message includes a number of required signatures and required principals, where the number may be used in determining whether to apply a configuration command. Moreover, while in paragraph [0069] BOSLER may be describing that a management server may be capable of sending management requests to the nodes being

managed, BOSLER does not describe that the management server checks or otherwise determines anything about a number of required signatures and required principals that are associated with a management request. In fact, it appears that paragraphs [0058] and [0069] of BOSLER refer to two completely different and separate embodiments – the embodiment in paragraph [0058] refers to establishing secure sessions between nodes by exchanging a management message, while the embodiment in paragraph [0069] refers to a management server that sends management requests to nodes that are being managed.

In contrast, Claim 1 comprises the features of receiving, in association with a particular configuration directive, security information defining a number of required signatures and required principals; and applying the particular configuration directive only when the configuration information has the number of required signatures by the required principals. According to these features of Claim 1, a particular configuration directive is applied only when the configuration information (which includes the particular configuration directive) has the number of required signatures and principals that is specified in previously received security information.

The Office Action asserts that in col. 3, lines 3-24, KINNIS describes the feature of Claim 1 of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the host network element. This assertion is incorrect.

In col. 3, lines 3-24, KINNIS describes a digital signature service that can be used by multiple users to sign a single document. A first user invokes the digital signature service to generate a first signature file corresponding to the document. After receiving the first signature file, a second user (e.g., a party to a contract with the first user) verifies through the digital

signature service that the content of document is not altered and authenticates the first user as the user who digitally signed the document. Then, if the second user wishes to digitally sign the document, the second user may invoke the digital signature service to generate a second signature file for the document.

Significantly, however, KINNIS does not describe or suggest anything about verifying whether the two users have collective authority to perform any configuration directives on a network element, as featured in Claim 1. While KINNIS may be describing that two users may digitally sign the same document, KINNIS does not describe or suggest that any verification is performed of whether the two user have collective authority to perform any action. Rather, KINNIS describes that any user who wishes to digitally sign the document may do so by using the digital signature service. (See, for example, KINNIS col. 9, lines 27-29, 41-45, and 53-54.) Thus, if anything KINNIS expressly teaches against verifying that two or more users have collective authority to perform an action. Furthermore, the users in KINNIS digitally sign documents but do not use the digitally signed documents to perform any action, such as applying configuration directives as featured in Claim 1. Rather, the users in KINNIS digitally sign the document in order to verify the integrity of the document and the authenticity of the users. (See, for example, KINNIS, col. 2, lines 32-36.)

In contrast, Claim 1 comprises the feature of verifying that the two or more digital signatures are valid and that two or more principals respectively associated with the two or more digital signatures have collective authority to perform the configuration directives on the network element. It is respectfully submitted that verifying the integrity of a document and authenticating the users that digitally signed the document (as described in KINNIS) is not equivalent to verifying that two or more principals have collective authority to perform configuration directives on a network element (as featured in Claim 1).

Finally, it is respectfully submitted that in order to sustain a rejection under 35 U.S.C. § 103(a), there must be some rational underpinning that supports the legal conclusion of obviousness. (See “Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.*”, published on October 10, 2007 in the Federal Register vol. 72, No. 195.) In the present rejection of Claim 1, however, there is no rational reason or other evidentiary underpinning for modifying the BOSLER system to use multiple digital signatures as described in KINNIS. Since BOSLER describes using a digital signature for the purpose of authenticating a sender node, the sender node does not need to send more than one signature in order to authenticate itself with the receiving node. In fact, BOSLER does not describe or suggest that a node may be assigned more than one private key, which means that in BOSLER a node CANNOT sign a management message with more than one digital signature. Thus, one of ordinary skill in the art would have absolutely NO reason, need, or rationale whatsoever for modifying the BOSLER system to use multiple digital signatures as described in KINNIS.

For the above reasons, BOSLER and KINNIS do not describe or suggest all features of Claim 1. Thus, Claim 1 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Reconsideration and withdrawal of the rejection of Claim 1 is respectfully requested.

B INDEPENDENT CLAIM 8

Claim 8 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. The rejection is respectfully traversed.

As a preliminary matter, it is noted that in rejecting Claim 8 the Office Action does not refer or cite to KINNIS. Further, the Office Action does not provide any response to the previously filed arguments, in which the Applicant argued that BOSLER does not describe or

suggest all features of Claim 8. For this reason, the Applicant respectfully submits that Claim 8 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS.

Among other features, Claim 8 comprises the features of:

receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or more particular configuration directives;

...;

only when the date-time value is within the time period and the one or more configuration directives have not been previously received during the time period, attempting to verify the one or more digital signatures based on the trust information, and applying the configuration directives to a network element only when the one or more digital signatures are verified successfully.

The Office Action asserts that the above features of Claim 8 are described in paragraphs [0071] and [0073] of BOSLER. This assertion is incorrect.

In paragraph [0071], BOSLER states:

The certification server 13 is arranged to receive a certificate-grant request and to issue the requested public-key certificate, provided that the time interval between the initialization time and the request time (i.e. the time when the certificate-grant request was received at the certification server 13) is within a maximum time interval 14 stored, for example, in the certification server 13. The time interval 14 is configurable by an authorized user, e.g. a network operator. In order to decide whether the certificate is granted, the certification server accesses the management information database 12 and recalls the stored initialization time for the managed node 4 from which the certificate-grant request was received. (Emphasis added.)

The time interval described in the above paragraph is an interval within which a node must request a public key certificate. Significantly, a certificate server would grant a public key certificate to a node only if the node requests the certificate within a particular time interval after a management agent is initialized/installed on the node. (See also at least BOSLER, paragraph [0010]; paragraph [0073], lines 17-22.) Thus, the time interval described by BOSLER is used to determine whether or not a node would be granted a public key certificate.

In contrast, Claim 8 includes the feature of receiving configuration control information that includes a time period during which a valid digital signature is required for applying one or

more particular configuration directives. A time period during which a valid signature is required for applying a configuration directive on a network element (as featured in Claim 8) is completely different from a time interval used to determine whether or not a node would be granted a public key certificate (as featured in BOSLER).

Further, in paragraph [0058] BOSLER describes that a first node and a second node may establish a secure session by exchanging a management message that may be authenticated by a digital signature. However, BOSLER does not describe or suggest that a management message sent by the first node includes any time interval. In fact, there is absolutely nothing in BOSLER that describes or suggests that management messages exchanged between nodes may include any time intervals indicating that configuration operations specified in the messages can be applied on nodes only during these time intervals. In contrast, the time period featured in Claim 8 is used to determine whether verification of one or more digital signatures would be attempted and whether one or more configuration directives would be applied to a network element.

For the above reasons, BOSLER and KINNIS do not describe or suggest all features of Claim 8. Thus, Claim 8 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS. Reconsideration and withdrawal of the rejection of Claim 8 is respectfully requested.

C. INDEPENDENT CLAIM 18

Claim 18 was rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS.

Claim 18 includes features similar to the features of Claim 8 discussed above. Thus, Claim 18 is patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS for at least the reasons given above with respect to Claim 8. Reconsideration and withdrawal of the rejection of Claim 18 is respectfully requested.

D. INDEPENDENT CLAIMS 21, 25, AND 29

Claims 21, 25, and 29 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS.

Claims 21, 25, and 29 include features similar to the features of Claim 1 discussed above, except in the context of an apparatus and a computer-readable medium. Thus, Claims 21, 25, and 29 are patentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS for at least the reasons given above with respect to Claim 1. Reconsideration and withdrawal of the rejection of Claims 21, 25, and 29 is respectfully requested.

E. DEPENDENT CLAIMS 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42,
AND 44-47

Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 were rejected as allegedly unpatentable under 35 U.S.C. § 103(a) over BOSLER in view of KINNIS.

Each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 depends from one of independent Claims 1, 8, 18, 21, 25, and 29, and thus includes each and every feature of the independent base claim. Thus, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is allowable for at least the reasons given above for Claims 1, 8, 18, 21, 25, and 29. In addition, each of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those features is not included at this time. Therefore, it is respectfully submitted that Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 are allowable for the reasons given above with respect to Claims 1, 8, 18, 21, 25, and 29. Reconsideration and withdrawal of the rejections of Claims 4-7, 9-17, 19-20, 23-24, 27-28, 31-32, 34-37, 39-42, and 44-47 is respectfully requested.

III. CONCLUSION

The Applicants believe that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicants respectfully submit that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the amendments and remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firms check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: May 23, 2008

/StoychoDDraganoff#56181/
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076